Utilizing Artificial Intelligence, Data Analytics, and Machine Learning to Strengthen Cybersecurity Infrastructure

Analyzing Cybersecurity Infrastructure in the United States: Effectiveness of the Current Structure

A Thesis Prospectus
In STS 4500
Presented to
The Faculty of the
School of Engineering and Applied Science
University of Virginia
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Science

By
Andrew Chau

May 9, 2023

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

ADVISORS

Kathryn A. Neeley, Department of Engineering and Society

Rosanne Vrugtman, Department of Computer Science

OVERVIEW

My connection to this technical project is that I am a Computer Science major and currently taking a cyber security class which constantly touches on situations like these about attackers targeting companies and systems to extract money or personal data. The methodology I will take is looking at real life examples or case studies and seeing how companies or the government have either responded or not responded to these vulnerabilities. My research question is how secure are energy, water, or sewage systems to cyber attacks? 1 thing readers will learn from my work is how vulnerable we all are digitally (no matter how big or small) nowadays since we put lots of trust in large companies to have a high level of cyber security, however, it is not as great as we think.

PROBLEMATIZATION

The problem I will be addressing is a lack of strong cyber and digital security infrastructure in large scale energy, water, or sewage systems. The main actors are the people using these systems, cyber attackers, and the companies managing these systems (either public or private entities). There will be a heavy focus on the societal aspect of this situation where the people are the ones who are hurt and affected by these vulnerabilities since attackers exploit people's safety for their own benefit. This stems from the fairly recent news of a string of cyber attacks within the past 2 years where power grids or water treatment facilities were shut down and hacked into by attackers that demanded ransom.

GUIDING QUESTION

How do cyber security infrastructure and management gaps in large scale energy, water, or sewage systems impact the community?

PROJECTED OUTCOMES

A policy change that I think should be implemented is a heavier punishment for cyber related crimes and the government should give subsidiaries and more resources to companies in order to encourage them to build up their cyber infrastructure. Additionally, there should be new regulations on a certain threshold in security levels that companies are required to have (a bare minimum) and if they don't meet that criteria they can be fined since people's private information and safety could be easily compromised. Oftentimes, problems are not talked about or widely known to the public and that is how accountability can be lost or ignored where the people's safety is not the first priority for many companies. Therefore, users of these systems (society) would immensely benefit from a deep dive on this topic since it shines a light on how companies can and should do better in order to prevent potential catastrophes from happening.

TECHNICAL PROJECT DESCRIPTION

My proposed technical project is that I will create a sort of "experiment" where in a controlled environment I will test out cyber security measures by building them to see how easy or not it would be to defend against common cyber threats and then elevating the threat levels. This also combines with my skills I learned from software testing where there would be a good amount of tweaking and fiddling with my code throughout the process. The point of my technical project is to simulate a small-scale version of a company implementing new security measures and I feel that my firsthand experience will help me better understand why some companies may be skimping on upgrading their systems due to constraints such as time, money, resources, etc. One last side note, I run a YouTube channel that posts singing videos and the point in bringing this up is how it showcases the idea where "technology can be used for good" since lots of people find comfort from my videos (and leave comments telling me so). This ties back to the point of human action defining technology (not the other way around) since in this case I control the effect technology has in influencing people where it is done in a positive manner rather than negative.

PRELIMINARY LITERATURE REVIEW & FINDINGS

Other engineers have given their own input into this issue about how to potentially mitigate these cyber vulnerabilities by having collaboration between different sectors or countries since it would create more synergy in combating threats. In one of the articles, it describes a collaboration between the US and Israel where the large-scale research had five projects but was able to be divided up due to the number of people collaborating. “The Israel-U.S. Initiative on Cybersecurity Research and Development for Energy, or ICRDE, was born from a proposal Weng submitted two years ago… The center was approved and formally began work in 2021… the researchers strategized smaller projects to achieve the coalition’s goals of conquering cybersecurity threats.” (Triolo, 2022). Additionally, the US government under the Biden administration has taken on some responsibility in establishing more resources dedicated to dealing with these cyberattacks such as more funding, a Cyber Safety Review Board, and promoting cybersecurity information sharing between the government and the private sector. “The budget request seeks $13.5 billion for cyber activities, a 20.5% increase from the previous year. The activities include implementing a zero-trust framework department-wide, advancing next-generation encryption solutions, funding five additional Cyber Mission Force teams and increasing cybersecurity support to the Defense Industrial Base (DIB) through the Cybersecurity Maturity Model Certification (CMMC) program.” (Sybert, Obis, Henderson, et al., 2023). “The Secretary of Homeland Security, in consultation with the Attorney General, shall establish the Cyber Safety Review Board” (Biden, 2021). Overall, I feel that the biggest challenge is funding as many companies do not feel the need to invest in cyber security infrastructure if they are not given any incentive to do so.

STS PROJECT PROPOSAL

STS is about how science and technology influences society based on things like how they emerge, how they change through social processes, etc. This is an STS project since cyber attacking these systems deal heavily with ethics because changing things like chemical levels in the water or shutting off power for a long period of time can cause people harm or death. It addresses why we should care about patching these holes in cyber security since it no longer deals simply with companies losing money but people and their lives.

I am approaching this problem from an ethics and values standpoint since a lack of digital security in these systems can affect hundreds of thousands (if not millions) of people where their safety is at serious risk (and even in serious cases, death). This brings up the question of whether we are putting too much trust and faith into companies / “the system”? The primary author I will be using is Foucault since he talks about how knowledge and power tie together and are not separate since in this case the cyber attackers use their “knowledge” of manipulating technology to hold power over the companies and people in order to get what they want (money, information, etc.). I feel that his viewpoint or theory ties very well to my problem about people abusing technology for their own personal agendas and how this lack of cybersecurity harms people immensely.

The approach that I will be using to investigate my problem is the value sensitive design since suggesting or proposing new policy or changes can be based on the values of the community (society). A potential value or belief of the community is that technology doesn’t define human actions, but rather the other way around. Therefore, stricter laws to deter people choosing to manipulate technology for their own personal gains should be enacted rather than punishing the technology itself by putting unnecessary limitations on it. Selfish desires have always existed prior to technology and did not just appear all of a sudden because of the rise of technology, that is why there are many laws added over time to keep up with the changing times. I think this will co-produce research that aligns with my definition and understanding of STS above where a lack of ethics of some people forces the “design” of needing more rules and regulations in place to protect the people and keep people on a “level playing field”. Also, it plays into the idea that people who “have more knowledge” about manipulating these technologies than others use it to take advantage of those who are not as well knowledgeable and abuse this power (Foucault).

One of my anticipated methods is doing case studies of real-life cases (such as the Colonial Pipeline ransomware attack) since the best way to learn about the lack of cyber security in energy infrastructure is to review recent documented experiences of cyber attacks around the world (not just the US). Analyzing these situations showcase the insecurities and loop holes these systems face and what could be done in the future to prevent or better handle these weaknesses, the best way to learn from mistakes is from the mistakes themselves.

BARRIERS & BOONS

Potential blind spots and limitations is that this topic in some respect is fairly new and everchanging, so the data that is out there might be recent but already outdated since technology and cyber attackers move quickly. I personally have no experience in the work force in regard to computer science or cyber security, this could limit my credibility as an author where I would want to find someone who has experience in the field and can back up my claims and research.

Additionally, there is not extensive history or data to reference or talk about since the US government has only recently started to act and insert themselves into these issues. I can offset these problems by trying to find sources that are as recent as possible and ones that are firsthand experiences from people in the field since they can give a better detailed insight.

REFERENCES

“ASU Researchers Collaborate Internationally to Secure Power Grid.” *ASU News*, 14 Dec. 2022, https://news.asu.edu/20221214-asu-researchers-collaborate-internationally-secure-power-grid.

"Biden's 2024 Budget Impacts IT Modernization Across Government." *GovernmentCIO Media*. https://governmentciomedia.com/bidens-2024-budget-impacts-it-modernization-across-government

"Executive Order on Improving the Nation’s Cybersecurity." *The White House*. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/